FedRAMP Forward Continuous Monitoring White Paper

Version 1.0

February 28, 2015

Table of Contents

List of Tables

1. INTRODUCTION

Under the Federal Information Security Management Act (FISMA) of 2002 and the guidance from the Office of Management and Budget (OMB) Circular A-130, Federal Agencies are required to reauthorize Federal computer systems at least every three years. However, with the release of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, NIST SP 800-37, OMB Memorandum M-14-03, OMB Memorandum M-14-04, NIST's Supplemental Guidance on Ongoing Authorization and the implementation of the Continuous Diagnostics and Mitigation program (CDM), the Federal Government is moving away from the annual 1/3rd, re-authorization every 3 years approach towards a risk-based model, where authorization of a system depends on ongoing assessments of the system's risk posture.

Considering these factors, the Federal Risk and Authorization Management Program (FedRAMP) will need to update its processes and consider new capabilities to ensure that FedRAMP authorizations keep pace with both the new Federal requirements and the evolving approach to security.

2. CURRENT APPROACH

The current FedRAMP Continuous Monitoring approach is detailed in "FedRAMP's Evolving Approach to Continuous Monitoring" paper. This paper provides a high level overview of the current approach-

1. Created to comply with past FISMA and OMB requirements by using a testing strategy that requires testing approximately 1/3 of the security controls annually in order to reauthorize the system every 3 years.
2. Focuses on compliance with requirements instead of focusing on an assessment of risk.
3. Core controls used for continuous monitoring are focused on requirements for testing over time, not specific risks presented by the cloud service provider's (CSP) system.
4. Provides oversight of the compliance of the CSP's system but doesn't provide much insight into how the system is actually performing.
5. Continuous monitoring deliverables are provided on a monthly basis instead of giving a near real-time picture of the system's risk posture.
6. The process is very resource intensive for the CSP and the Authorizing Official (AO).
7. The high level of effort required for FedRAMP to perform continuous monitoring for P-ATO packages means that the process is difficult to scale up to monitor a large number of CSPs.

8. FedRAMP's current continuous monitoring program does not incorporate new requirements and tools to automate continuous monitoring and reporting, such as the COTS tools available through CDM.

3. MOVING CONTINUOUS MONITORING FORWARD

In order to move the FedRAMP continuous monitoring program forward, FedRAMP program management office (PMO) created a strategic and long term plan to guide the evolution of the continuous monitoring program within FedRAMP. This five step plan has the overall goals of:

1. Implementing risk based testing and assessment by focusing on areas of high risk
2. Alleviating the burden on CSPs and 3PAOs presented by continuous monitoring by reducing the number of controls needing to be assessed. This would be dependent on CSPs past and present performance related to POAM remediation and tracking.
3. Providing better insight into the security posture the cloud system by moving toward automation of continuous monitoring to provide a near real-time picture of the system.

The steps of the plan are:

1. Analysis of current continuous monitoring core controls
2. Performance driven analysis of continuous monitoring data
3. Establish CSP continuous monitoring and testing profiles
4. Assessment of automated continuous monitoring tools and CDM requirements
5. On-going updates of FedRAMP requirements, testing requirements, templates and guidance.

Each of process steps are provided below with additional detail.

3.1. ANALYSIS OF CURRENT CONTINUOUS MONITORING CORE CONTROLS

The FedRAMP *Continuous Monitoring Strategy and Guide* currently lists core controls that must be assessed or performed as part of the CSP's continuous monitoring plan and annual assessment. These controls were selected based on the frequency set by the requirements in the control, such as if the control has a requirement that must be met on a continual basis, weekly, monthly, quarterly, annually or every three years. For example the information system inventory must be monitored continually based on control CM-8(3) and RA-5 requires that vulnerability scans are performed and the results sent to the ISSOs monthly.

While these controls are helpful in providing a picture of the CSP's system in terms of complying with FedRAMP requirements, they were not selected to provide a clear picture of the actual or real risk posture of the CSP's system.

In order to provide a clearer picture of the actual risk presented by the CSP's system, the development team recommends reviewing the core controls with the intent of selecting controls that specifically target risk in the CSP's system and provide the most impact in assessing whether the system's risk posture meets FedRAMP's criteria. As part of this analysis, FedRAMP may want to look at some other standards in selecting new controls such as the SANS Top 20 Critical Controls.

By focusing on risk, FedRAMP may be able to reduce the number of core controls and thus reduce the amount of resources that both the CSP and the FedRAMP program management office (PMO) must dedicate to continuous monitoring.

3.2. PERFORMANCE DRIVEN ANALYSIS OF CONTINUOUS MONITORING DATA

The implementation of the automated Scan Center tool provides an opportunity to take the analysis of continuous monitoring controls a step further by reviewing and analyzing the continuous monitoring data provided by each FedRAMP compliant CSP. By analyzing the data FedRAMP can identify specific areas of risk based on actual data.

This analysis provides further benefits by allowing FedRAMP to:

1. Provide a way to validate the selection of the core controls and possibly further narrow or focus the core control selection
2. Identify specific areas of high risk in the CSP's system which may need additional scrutiny
3. Help identify different areas of risk based on cloud deployment model, service model, service provided, and specific to the service provider
4. Provide the flexibility to create a set of core controls that account for a CSP's delivery model and service provided
5. Provide an opportunity to move away from the 1/3 testing methodology since the control selection for annual assessments are focused on risk and not compliance

3.3. ESTABLISH CSP CONTINUOUS MONITORING AND TESTING PROFILES

Upon assessment of a CSPs continuous monitoring data, FedRAMP will be able to develop a risk profile for each CSP that is customized based on risk and problem areas, while also identifying areas where the CSP has demonstrated a high level of compliance and a lower level of risk.

In addition, FedRAMP should also use this information to create generic core control and testing profiles for CSPs based on its delivery model and the service provided. For example an email as a service SaaS may have a slightly different continuous monitoring and testing profile than a SaaS offering a remote desktop service.

This information would be used by the FedRAMP PMO to develop a specific testing approach and assist with control selection for the annual assessment and will replace the current 1/3, 1/3, 1/3 approach for testing. This customized control selection presents an opportunity to reduce the testing burden for CSPs for continuous monitoring and annual assessments. For example, if the CSP has demonstrated a high level of compliance and lower risk for certain controls, the customized risk profile and testing approach would be focused mainly on areas of risk, and may remove the requirement to re-test some controls.

In addition to using a risk based selection of controls for annual testing this testing strategy would also incorporate a mix of random controls for testing during annual assessment. The inclusion of random controls will help ensure that the CSP is considering total risk posture and can't just focus on list of controls for annual testing.

3.4. ASSESSMENT OF AUTOMATED TOOLS AND CDM REQUIREMENTS

Automation of the continuous monitoring for the CSPs would decrease the testing burden for CSPs, reduce the burden for ISSOs in terms of the requirement to review monthly deliverables and would provide insight into whether the control implementation is effective. Automation would also allow FedRAMP to move towards ongoing assessments since these tools can provide a near real-time view into the system. In addition, if properly implemented, automation opens the door for using data feeds from the tools to populate a dashboard which could provide a global view of CSP status across all FedRAMP compliant systems.

FedRAMP should review the FedRAMP baseline and the current offering of available COTS tools to produce an analysis of the controls that can be automated and enable CSPs to provide the information needed to demonstrate that a control is implemented and working properly. One study estimated that approximately 32% of NIST SP 800-53 controls can be automated; however, there are still management and operational controls,

such as Awareness Training, Maintenance, Planning and Personnel Security that do not lend them to automation at this time[1].

FedRAMP will also need to review the new CDM requirements and COTS tools and determine which tools are suitable for use for FedRAMP compliant CSPs, determine which controls may be automated using CDM tools and the acceptable implementation of these tools for FedRAMP. This analysis would allow CSPs and agencies to select tools offered through CDM to satisfy FedRAMP requirements.

The analysis should also include forward looking analysis to identify the elements and technology needed to expand the number of controls that can be automated within the FedRAMP program. The analysis would also need to look into data schema that would be required to allow the transmission of information to FedRAMP in a standardized form, to allow CSPs to use a wide range of programs and tools within their system. FedRAMP may also want to consider looking at the feasibility of selecting tools that FedRAMP would require CSPs to use in order to receive a reduction in continuous monitoring requirements.

Based on the feedback from the "FedRAMP's Evolving Approach to Continuous Monitoring" paper, the following tools maybe considered:

Tool	Notes / Controls Automated
Telos Xacta	Risk and Compliance (GRC) tool
RSA Archer	Risk and Compliance (GRC) tool
ArcSight Monitoring & Management Service	Assists the CSP in meeting the following FISMA Controls: AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12AC-2(4), AC-17
HP Tipping Point Intrusion Prevention System Monitoring Service	Assists the CSP in meeting the following FISMA Controls: SI-4, SI-4(1), SI-4(2), SI-4(3), SI-4(4), SI-4(5), SI-4(6), SI-5AC-4, AC-5, AC-17
McAfee ePolicy Orchestrator	Assists the CSP in meeting the following FISMA Controls: SI-3, SI-3(1), SI-3(2), SI-3(3), SI-5, SI-7, SI-7(1), SI-7(2)CM-6, CM-6(1), CM-6(2), CM-6(3), CM-6(4), CM-7, CM-7(2)
Retina CS Vulnerability Management Console	Assists the CSP in meeting the following FISMA Controls: CM-2(4), CM-2(5), CM-4(2), CM-8(3),RA-5, RA-

[1] Raydel Montesino and Stefan Fenz, "Information security automation: how far can we go," in Sixth International Conference on Availability, Reliability and Security, 2011, pp. 280-285.

	5(1), RA-5(2), RA-5(3), RA-5(4), RA-5(5), RA-5(7)SI-2, SI-2(2), SI-5
Cloud Security Automation Code (CSAC)	Concept of the tool is to develop human readable, machine-executable code that will automatically configure cloud systems to meet FedRAMP requirements for low or moderate security impact levels.

Table 1.1 Feedback on Automated Tools from the "FedRAMP's Evolving Approach to Continuous Monitoring" paper

While this is not an exhaustive list, it provides a starting point for consideration of tools. In addition to the review of tools, FedRAMP may also want to consider how the data for these tools may be integrated into a workflow tool used by FedRAMP. The workflow tool Request for Information (RFI) will be released as part of the FedRAMP forward plan.

3.5. ON-GOING UPDATES OF FEDRAMP REQUIREMENTS, TESTING REQUIREMENTS, TEMPLATES AND GUIDANCE.

As the requirements and tools for continuous monitoring evolve, so will the requirements, guidance and the templates.

Any significant changes to the FedRAMP requirements or policies for continuous monitoring will require a re-write of the *FedRAMP Continuous Monitoring Strategy and Guide*, impact the Security Assessment Plan (SAP), annual SAP, Security Assessment Report (SAR), and may lead new guidance or documents to cover issues such as automation.

In addition to considering any changes that may come from the CDM program, FedRAMP should also anticipate the next NIST revision for 800-53, which will require major updates to the majority of FedRAMP documents. Since NIST and the Department of Homeland Security have made major shift towards focusing on continuous monitoring and on-going authorizations, the development team would guess that we may see some of the same themes in any updates to 800-53. These changes would have a major impact on the System Security Plan template, *FedRAMP Continuous Monitoring Strategy and Guide*, and also require an update to the transition strategy for migrating and testing the updated baseline during annual assessments. The FedRAMP PMO will need to review the transition testing strategy to determine if evidence from the previous control set could be used to satisfy the requirements of the updated FedRAMP baseline and test cases.